## CSE 417: Algorithms and Computational Complexity

Winter 2002
Justin Campbell

## Russell's Paradox

- Similar in flavor to the Halting problem.
- Consider the set of all sets that don't contain themselves.
|l Example: $\{a, b,\{a\}\}$
|| Does this set contain itself?


## Reductions

| We write: $L \leq R$

- We transform an instance of $L$ into an instance of $R$ such that R's answer is L's.
| Function $\mathrm{L}(\mathrm{x})$
Run program $T$ to translate input $x$ for $L$ into an input $y$ for $R$
Call a subroutine for problem $R$ on input $y$ Output the answer produced by $R(y)$


## Reductions

II If $L \leq^{p} R$ and $R$ is efficiently solvable then so is $L$. Using the contrapositive, if $L$ is provably slow, then $R$ must be.

II If $L$ is $\Omega(P(n))$ and the reduction is $T(n)$ then $R$ is $\Omega(P(n)-T(n))$

## Reductions Exercise

## Properties of polynomial-time

 reductions|| Theorem: If $L \leq^{p} R$ and $R \leq^{p} S$ then $L \leq^{p} S$
Given an undirected graph $\mathrm{G}=(\mathrm{V}, \mathrm{E})$ and an integer k is there a subset W of V of size at most k such that every edge of G has at least one endpoint in W? (i.e. W covers all vertices of G).
|| Independent-Set:
\| Given a graph $G=(V, E)$ and an integer $k$, is there a subset $U$ of $V$ with $|\mathrm{U}| \geq \mathrm{k}$ such that no two vertices in U are joined by an edge.

Proof idea:
I Compose the reduction $T$ from $L$ to $R$ with the reduction $T^{\prime}$ from $R$ to $S$ to get a new reduction $T^{\prime \prime}(x)=T^{\prime}(T(x))$ from $L$ to $S$.

## Computational Complexity

I. Classify problems according to the amount of computational resources used by the best algorithms that solve them

## I Define:

l $\operatorname{TIME}(f(n))$ to be the set of all problems solved by algorithms having worst-case running time O(f(n))
Ex: Sorting is in TIME(nlogn).

## Polynomial time

Define $P$ (polynomial-time) to be
I the set of all problems solvable by algorithms whose worst-case running time is bounded by some polynomial in the input size.
$\mathrm{P}=\mathrm{U}_{\mathrm{k} \geq 0} \operatorname{TIME}\left(\mathrm{n}^{\mathrm{k}}\right)$

## Beyond P?

1 There are many natural, practical problems for which we don't know any polynomial-time algorithms

II e.g. Vertex-Cover, Independent-Set
II e.g. Traveling Salesman Problem
II e.g. Satisfiability

## Satisfiability

|| Boolean variables $\mathrm{x}_{1}, \ldots, \mathrm{x}_{\mathrm{n}}$ I taking values in $\{0,1\}$. $0=$ false, $1=$ true
I. Literals
$\| x_{i}$ or $\neg x_{i}$ for $i=1, \ldots, n$

- Clause

I a logical OR of one or more literals
e.g. $\left(x_{1} \vee \neg x_{3} \vee x_{7} \vee x_{12}\right)$

- CNF formula

I a logical AND of a bunch of clauses

## Satisfiability

1 CNF formula example
$1\left(x_{1} \vee \neg x_{3} \vee x_{7} \vee x_{12}\right) \wedge\left(x_{2} \vee \neg x_{4} \vee x_{7} \vee x_{5}\right)$
II If there is some assignment of 0 's and 1 's to the variables that makes it true then we say the formula is satisfiable
II Is the following formula satisfiable?
$x_{1} \wedge\left(\neg x_{1} \vee x_{2}\right) \wedge\left(\neg x_{2} \vee x_{3}\right) \wedge \neg x_{3}$
Satisfiability: Given a CNF formula F, is it satisfiable?

## Common property of these hard problems

\| There is a special piece of information, a short hint or proof, that allows you to efficiently verify (in polynomial-time) that the answer is correct. This hint might be very hard to find.

Ille.g.
II Independent-Set, Clique: the set of vertices
I Satisfiability: an assignment that makes F true.

## The complexity class NP

NP consists of all problems where one can verify the answers efficiently (in polynomial time) given a short (polynomial-size) hint.

The only obvious algorithm for most of these problems is brute force:
I try all possible hints and check each one to see if it works.
| Exponential time.

## Unlike undecidability

Nobody knows if all these problems in NP can all be done in polynomial time, i.e. does $P=N P$ ?
I one of the most important open questions in all of science.
| huge practical implications
How are P and NP related?

## $P$ and NP



## NP-hardness \& NP-completeness

- Alternative approach

I show that they are at least as hard as any problem in NP

Rough definition:
\| A problem is NP-hard iff it is at least as hard as any problem in NP
| A problem is NP-complete iff it is both
NP-hard
in NP

## NP-hardness \& NP-completeness

|l Definition: A problem R is NP-hard iff every problem $L \in N P$ satisfies $L \leq^{p} R$

II Definition: A problem R is NP-complete iff $R$ is NP-hard and $R \in N P$

- Not obvious that such problems even exist!

